Zero Day Exploit

ANIMESH KUMAR

Student of NLIU, Bhopal

Contact Details:

Mail: kumar.animesh91@gmail.com

Mobile: +91-9713914470

Skype: animeshkumarr

Electronic copy available at: https://ssrn.com/abstract=2378317
Electronic copy available at: http://ssrn.com/abstract=2378317

ABSTRACT

Zero day vulnerability is vulnerabilities against which no vendor has a patch and no one has still released any patch in the market. Due to the absence of patch it's a major threat to the concern organization and its users. Zero day exploit is the day between the vulnerability is known and the first day of its attack. Nowadays there are a good number of security expert in the market so the common vulnerabilities are rare and it can be easily patch. Before the vulnerability was of buffer overflow kind but in present scenario it's mainly of logical errors and due to lack of configuration in the security. This misconfigutaion is because of mainly three reasons:

- Due to lack of knowledge: this may occur if the security analyst doesn't have sufficient knowledge about all the related patches.
- Due to overconfidence of the security analyst: he assumes that the hacker/crackers can't breach security of this level and this illusion affects the organization at large.
- Due to lack of interest while implementing the security mechanism: this happens due to some personal or professional reason that the security analyst mere implement security mechanism.

These bugs can be detected in following ways:

- By using early detection techniques such as IPsec, stateful firewall, protected Wi-Fi access such as WPA2
- By trying each and every possibility on a web application
- By analyzing the source code and focus on the single point of any web application

Electronic copy available at: https://ssrn.com/abstract=2378317
Electronic copy available at: http://ssrn.com/abstract=2378317

INTRODUCTION

A zero day exploit is vulnerability when one takes the advantage of the security vulnerability and those becomes the well known vulnerability when it's discovered and when it is attacked for the first time. Since the vulnerability is discovered for the first time so there is no known solution or patches for it and thus it can be exploited till the vulnerability got patched. For some early detection of the vulnerability, organizations some techniques such as virtual LAN, Intrusion Detection System (IDS), Intrusion Protection System (IPS), protected Wi-Fi access mainly WPA2 as it uses hard encryption techniques and the key is encrypted 4096 times.[1]

METHODOLOGY

Zero day vulnerability, a sub set of total no of documented vulnerability reported over a particular spam of time. It is a vulnerability that is exploited before it is known publically. It may not have been known to the affected vendor prior to exploitation and, at the time of the exploit activity, the vendor had not released a patch[2].

Fig. 1

[1] Source http://searchsecurity.techtarget.com/definition/zero-day-exploit, Visited on 12/01/2014
[2] Source http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities, Visited on 12/01/2014

Electronic copy available at: https://ssrn.com/abstract=2378317

Figure D.5

Zero-Day Vulnerabilities Identified In 2011

CVE Identifier	Description
CVE-2011-0609	Adobe Flash Player 'SWF' File Remote Memory Corruption Vulnerability
CVE-2011-0611	Adobe Flash Player 'SWF' File Remote Memory Corruption Vulnerability
CVE-2011-1255	Microsoft Internet Explorer Time Element Remote Code Execution Vulnerability
CVE-2011-1331	JustSystems Ichitaro Memory Management Program Remote Heap Buffer Overflow Vulnerability
CVE-2011-2107	Adobe Flash Player Cross-Site Scripting Vulnerability Alert
CVE-2011-2462	Adobe Reader/Acrobat U3D Memory Corruption Vulnerability
CVE-2011-3402	Win32k True Type Font Parsing Vulnerability
CVE-2011-3544	Oracle Java Rhino Script Engine

Source: Symantec

Fig. 2[3]

PROCESS OVERVIEW

Process overview covers the entire portion regarding the participant those who are the intended to find the vulnerability and are reported and it also covers phases from finding to its patch releasing.

PARTICIPANTS:

- The finder

  One, who finds the vulnerabilities, may be a scholar, researcher, security expert, customer or any other interested person in the arena of security.
- The vendor

  One, who develops the product, may be any organization, firm or individual who has the responsibility to maintain the security of the product.
- Coordinator

  The person, serve as a proxy participant to find the vulnerability mainly of technical vulnerabilities to promote the effectiveness for the process of security.

[3] Source http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities, Visited on 12/01/2014

Electronic copy available at: https://ssrn.com/abstract=2378317

- Arbitrator

  The person acts as an adjudicating officer between the finder and the vendor to resolve the dispute.

PHASES:

- Discovery

  The finder discovers the flaw in the process and is known as the discovery of security vulnerability.

- Notification

  In this step the finder finds the flaws and notifies the concern person and the vendor in return confirms that he received the notification.

- Investigation

  The vendor investigate the flaws that are been reported and notified by the finder and validate the finders claim and works on the vulnerability to patch it.

- Resolution

  When the flaw is confirmed then the vendor develops solution for the particular vulnerability so that the effect can be nullified or minimized.

- Release

  After all the desired steps are completed then the vendor releases the information publically for the patch of the vulnerability.[4]

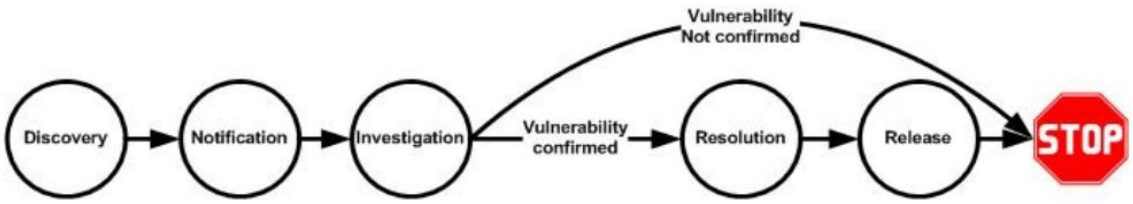

Fig. 3[5]

[4] Source http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf, Visited on 12/01/2014

[5] Source http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf, Visited on 12/01/2014

Electronic copy available at: https://ssrn.com/abstract=2378317

CONCLUSION

Thus it is concluded that for searching the vulnerability by trying each and every possibility the security expert must be aware of all types of vulnerability so that he can check all the possible security for all types of attack. For analyzing of the source code the security expert must be aware of all types of the tools or reverse engineering and he must also be aware of the development part of the source code so that he can easily detect the flow of the code.

To start with there are two ways that either it may affect the client side or the server side else it may also depend that it may be of network side or web application side. The exploit may be represented in these ways, if the vulnerability is based on the web application then the expert design the payload or request header or request query and if the vulnerability is software based then the expert will patch it with the help of Perl python or c language.

Electronic copy available at: https://ssrn.com/abstract=2378317